Sorbonne Université

Entiers de Gauss

Norman El Fartass *Esteban Wahler* *Seoyeon Shin*

Marco Maculan

Leonardo Zapponi

Introduction historique

La première mention des entiers de Gauss fut en 1801 par Carl Friedrich Gauss (1777-1855) lui-même. Il y fit part de contributions importantes en arithmétique. Ces contributions, notamment pour la notation des congruences, lui permirent de prouver à l'âge de 18 ans, à l'aide de ce nouveau type "d'entiers", l'un des théorèmes les plus importants de son temps. Il s'agit de la loi de réciprocité quadratique, surnommée le "théorème d'or", qui avait d'abord été conjecturée par Euler puis reformulée par Legendre.

Une tentative de généralisation de la méthode de Gauss pour résoudre le cas quadratique débouche dans le cas cubique avec les entiers d'Eisenstein de la forme :

$$z = a + \omega b$$

Où a et b sont des entiers relatifs et $\omega = e^{2\pi i/3}$. La généralisation débouche également dans le cas des puissances cinquième avec $\mathbb{Q}[\sqrt{5}]$. L'étude de ces structures a ensuite permis le développement de la notion d'anneaux avec notamment les travaux de Richard Dedekind, David Hilbert ou encore Emmy Noether.

Aujourd'hui, on recense près de 345 preuves de la loi de reciprocité quadratique. Établir une loi de réciprocité dans les corps de nombres est encore aujourd'hui un problème ouvert (9-ème problème de Hilbert) et une partie de cette généralisation a conduit à la théorie des corps de classes.

Table des matières

1 Structure de $\mathbb{Z}[i]$

Dans ce papier, on s'intéresse à l'ensemble $\mathbb{Z}[i] \coloneqq \{a + ib,\ a, b \in \mathbb{Z}\}$.
Montrons dans un premier temps que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$. On a tout d'abord $0 = 0 + 0i \in \mathbb{Z}[i]$ et $1 = 1 + 0i \in \mathbb{Z}[i]$. Soient $z \coloneqq a + ib \in \mathbb{Z}[i]$ et $z' \coloneqq a' + ib' \in \mathbb{Z}[i]$. Alors

$$z + z' = a + ib + a' + ib' = \underbrace{(a + a')}_{\in\mathbb{Z}} + i\,\underbrace{(b + b')}_{\in\mathbb{Z}} \in \mathbb{Z}[i].$$

De même, on a

$$zz' = (a + ib)(a' + ib') = aa' + aib' + a'ib + i^2bb' = \underbrace{(aa' - bb')}_{\in\mathbb{Z}} + i\,\underbrace{(ab' + a'b)}_{\in\mathbb{Z}} \in \mathbb{Z}[i].$$

Ce qui montre finalement que $\mathbb{Z}[i]$ est un bien un sous-anneau de $\mathbb{C}$. C'est même un anneau à part entière, mais c'est plus fastidieux à montrer donc nous l'admettrons ici.

2 Anneau euclidien

Avant commencer à discuter plus de $\mathbb{Z}[i]$, on introduit la structure algébrique d'anneau euclidien.
On commence par quelques rappels :

Définition 2.1. (rappel). Un *anneau intègre* est un anneau A tel que, pour tous $a, b \in A$

$$ab = 0_A \implies a = 0_A \text{ ou } b = 0_A.$$

On pourra penser à $\mathbb{Z}/n\mathbb{Z}$, où n n'est pas premier, comme exemple d'anneau non intègre.

Définition 2.2. (rappel). Un *idéal principal* d'un anneau A est un idéal engendré par un seul élément de A. Un *anneau principal* est un anneau intègre dont tous les idéaux sont principaux.

Avec ces definitions en tête, on se permet de commencer à parler d'un anneau euclidien avec quelques exemples classiques.

Définition 2.3. Soit $(A, +, \cdot)$ un anneau commutatif intègre. A est dit *euclidien* s'il est possible d'y définir une division euclidienne.

Exemple 2.4.

- Entiers relatifs $\mathbb{Z}$
  On peut évidemment définir une division euclidienne "usuelle" par rapport à la valeur absolue :

  $$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0_{\mathbb{Z}}\},\ \exists q, r \in A,\ tels\ que\ a = bq + r\ \wedge\ |r| < |b|.$$

- Polynômes à coefficients dans un corps commutatif $\mathbb{K}$
  La division sur $\mathbb{K}[X]$ prend la forme suivante :

  $$\forall (A(X), B(X)) \in \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\},\ \exists!\ Q(X), R(X) \in \mathbb{K}[X],$$
  $$tel\ que\ A(X) = B(X)Q(X) + R(X)\ \wedge\ degR(X) < degB(X).$$

"Pouvoir définir la division euclidienne" peut sembler facile à dire, mais le problème apparait dans la dernière partie de la division euclidienne : "le reste de la division doit etre

strictement petit que le diviseur". Cela nous pose une question de la grandeur d'ordre de deux éléments. Mais comment peut-on définir la relation d'ordre sur ces anneaux et par rapport à quoi ? C'est le stathme euclidienne qui nous permet de répondre à cette question et de définir la notion d'un anneau euclidien plus rigorousement.

Définition 2.5. Un *stathme euclidien* sur un anneau A est une application $f : A \setminus \{0_A\} \implies \mathbb{N}$ telle que

1. $\forall (a,b) \in A \times A \setminus \{0_A\},\ \exists q, r \in A,\ a = bq + r$ où $r = 0$ ou $f(r) < f(b)$,
2. $\forall a, b \in A \setminus \{0_A\},\ f(a) \leqslant f(ab)$.

S'il existe une telle application, on dit que A est un *anneau euclidien*.

On termine par une proposition, dont la démonstration a été traitée en TD.

Proposition 2.6. (rappel). Tout anneau euclidien est principal.

C'est bien la principalité d'un anneau euclidien qui lui permet de posséder toutes les bonnes propriétés de divisibilités des anneaux principaux, à commencer par le théorème de Bezout, le lemme de Gauss et le lemme d'Euclide. Il est de plus atomique car toute suite croissante d'idéaux principaux est stationnaire. Il est factoriel ; c'est-à-dire qu'il vérifie le théorème fondamental de l'arithmétique. L'existence de telles propriétés sont exactement la raison pour laquelle on a envie de définir une division euclidienne sur l'anneau.

3 Propriétés de $\mathbb{Z}[i]$

3.1 Norme sur $\mathbb{Z}[i]$

Proposition 3.1.1. On pose

$$\begin{aligned} N\ :\ \mathbb{Z}[i] &\implies \mathbb{N} \\ z = a + ib &\longmapsto a^2 + b^2 \end{aligned}$$

l'application qui associe à tout entier de Gauss sa "norme". Alors, la norme N est multiplicative.

Démonstration. On a $N(zz') = |zz'|^2 = |z|^2 |z'|^2 = N(z)N(z')$. □

Proposition 3.1.2. On a $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Démonstration. Tout d'abord, 1 et -1 sont trivialement inversibles dans $\mathbb{Z}[i]$. De plus, $\dfrac{1}{i} = \dfrac{-i}{i(-i)} = -i \in \mathbb{Z}[i]$ et $\dfrac{1}{-i} = \dfrac{i}{-i^2} = i \in \mathbb{Z}[i]$. Réciproquement, si $z \in \mathbb{Z}[i]^*$, alors il existe $z' \in \mathbb{Z}[i]^*$ tel que

$$zz' = 1 \implies N(zz') = 1 \iff N(z)N(z') = 1$$

qui est un produit dans $\mathbb{N}$ égal à 1, ce qui implique que les deux entiers valent 1. En particulier on a $N(z) = 1$ soit $a^2 + b^2 = 1$ qui est l'équation de cercle $C\big((0,0),1\big)$. Or $\mathbb{Z}[i] \cap C\big((0,0),1\big) = \{\pm 1, \pm i\}$, ce qui conclut la preuve. □

Remarque. On appellera les éléments ± 1 et $\pm i$ des unités.

Lemme 3.1.3. Soit $z \in \mathbb{Z}[i]$ non nul. Les seuls entiers de Gauss de norme 1 ou de norme $N(z)$ qui divisent z sont $\pm z$ et $\pm iz$.

Démonstration. Si $\beta \mid z$ et $N(\beta) = 1$, alors β est une unité, *i.e.* $\beta = \pm 1$ ou $\beta = \pm i$.
Si $\beta \mid z$ et $N(\beta) = N(z)$, on pose $\gamma \in \mathbb{Z}[i]$ tel que $z = \beta\gamma$. Alors, on a $N(z) = N(\beta)N(\gamma)$. En simplifiant par $N(z) = N(\beta)$, on a $N(\gamma) = 1$ donc $\gamma = \pm 1$ ou $\gamma = \pm i$. Donc $\beta = \dfrac{z}{\gamma} = \dfrac{z}{\pm 1}$ ou $\dfrac{z}{\pm i}$, *i.e.* $\beta = \pm z$ ou $\pm iz$. □

3.2 Divisibilité sur $\mathbb{Z}[i]$

La divisibilité sur l'ensemble $\mathbb{Z}[i]$ est définie de manière habituelle : soient $\alpha, \beta \in \mathbb{Z}[i]$. On dit que β divise α ($\beta \mid \alpha$) s'il existe $\gamma \in \mathbb{Z}[i]$ tel que $\alpha = \gamma\beta$. On appelle alors β *un diviseur* (ou *un facteur*) de α.

Voici deux exemples :

Exemple 3.2.1. $4 - 5i \mid 7 - 19i$ car $(4 - 5i)(3 - i) = 7 - 19i$.

Exemple 3.2.2. On divise $7 - 19i$ par $3 + i$ en prennant le ratio et en rationalisant le dénominateur :

$$\frac{7 - 19i}{3 + i} = \frac{(7 - 19i)(3 - i)}{(3 + i)(3 - i)} = \frac{2 - 64i}{10} = \frac{1}{5} + \frac{32}{5}i.$$

Comme ce ratio n'est pas dans $\mathbb{Z}[i]$, $3 + i \nmid 7 - 19i$.

Théorème 3.2.3. Soit $\alpha = a + bi \in \mathbb{Z}[i]$. α est divisible par $c \in \mathbb{Z}$ si et seulement si $c \mid a$ et $c \mid a$.

Démonstration. On a :

$$\begin{aligned} c \,|\, a + bi &\iff \exists\, m,\, n \in \mathbb{Z},\, c(m + ni) = a + bi \\ &\iff a = cm \ \wedge\ b = cn \\ &\iff c \,|\, a \ \wedge\ c \,|\, b. \end{aligned}$$

□

Théorème 3.2.4. Soit $\alpha, \beta \in \mathbb{Z}[i]$. Si β divise α alors $N(\beta)$ divise $N(\alpha)$.

Démonstration. Soit $\gamma \in \mathbb{Z}[i]$. On a :

$$\begin{aligned} \alpha = \gamma\beta &\implies N(\alpha) = N(\gamma)N(\beta) \\ &\iff N(\beta) \,|\, N(\alpha). \end{aligned}$$

□

Remarque. La réciproque du théorème 3.2.4 est clairement fausse (c.f. exemple 2) ; le théorème nous dit simplement que la divisibilité de la norme dans $\mathbb{Z}$ suit la divisibilité dans $\mathbb{Z}[i]$. Néanmoins, c'est une critère utile pour montrer qu'un entier de Gauss n'est pas divisible par un autre.

Voici un corollaire du théorème 3.2.4 avec un exemple.

Corollaire 3.2.5. Soit $\alpha \in \mathbb{Z}[i]$. $N(\alpha) \equiv 0[2]$ si et seulement si $(l + i)$ divise α.

Démonstration.

— $\Longleftarrow$: Soit $\alpha \in \mathbb{Z}[i]$. Si $N(1+i) = 2$,

$$(1+i) \,|\, \alpha \implies N(\alpha) = 2k,\ k \in \mathbb{Z}.$$

d'après le théorème 3.2.4.

— $\Longrightarrow$: Soit $\alpha = a + bi \in \mathbb{Z}[i]$. On a :

$$\begin{aligned} N(\alpha) \equiv 0[2] &\iff a^2 + b^2 \equiv 0[2] \\ &\implies a^2,\, b^2 \ \textit{pair ou}\ a^2,\, b^2 \ \textit{impair} \\ &\implies a \equiv b[2]. \end{aligned}$$

Ainsi :

$$\begin{aligned} (1+i) \,|\, (a+bi) &\iff \exists\, c + di \in \mathbb{Z}[i],\ (1+i)(c+di) = (a+bi) \\ &\iff (c-d) + (c+d)i = a + bi \end{aligned}$$

On cherche pour c et d qui conviennent : c $= \dfrac{b+a}{2}$, d $= \dfrac{b-a}{2}$. Or, $a \equiv b[2]$; donc $a,\, b \in \mathbb{Z}$.
$\therefore\ (1+i) \,|\, \alpha$.

□

Exemple 3.2.6. $(1+i) \,|\, (1-i) \iff i(1-i) = 1 + i$ car $N(1+i) = 2$.

On finit cette partie avec quelques remarques du point de vue arithmétique et algébrique.

Remarque (arithmétique). Soit m, n $\in \mathbb{Z}$. Si |m| = |n| , alors $m \pm n$; autrement dit, si m et n ont la même valeur absolue alors ils sont multiples d'unité de l'un à l'autre. Sur $\mathbb{Z}[i]$, c'est faux : il existe $\alpha,\, \beta \in \mathbb{Z}[i]$ tel que $N(\alpha) = N(\beta)$ et $\alpha \neq \gamma\beta$ où $N(\gamma) = 1$. L'exemple le plus simple est sur les conjugés, i.e. $N(a+bi) = N(a-bi)$, mais $a - bi$ n'est pas de multiple d'unité de $a + bi$.

Remarque (algébrique). Sur $\mathbb{Z}$, la division n'est pas de relation d'ordre car elle n'est pas antisymétrique (On appelle de telles relations des relations de préordre). Or, si on quotiente $\mathbb{Z}$ par ses classes inversibles, i.e. sur $\mathbb{Z}/\mathbb{Z}^\times = \mathbb{Z}/\{\pm 1\}$, la division est bien une relation d'ordre. Sur $\mathbb{Z}[i]$, c'est pareil : lorsque sur $\mathbb{Z}[i]$ la division est une relation de préordre, $\mathbb{Z}[i]/\mathbb{Z}[i]^\times = \mathbb{Z}[i]/\{\pm 1,\, \pm i\}$ est bien ordonné. En conclusion, on peut dire que la division est une relation d'ordre au signe près sur $\mathbb{Z}$, à la mulplication par unités près sur $\mathbb{Z}[i]$. On peut définir les éléments irréductibles avec cette relation d'ordre.

Théorème 3.2.7. Les *éléments irréductibles* sur $\mathbb{Z}[i]/\mathbb{Z}[i]^\times$ sont les minimaux pour la division (On rappelle que les éléments irréductibles ne sont ni nuls ni inversibles, et leurs seuls diviseurs sont les inversibles et les éléments associés à eux-même).

3.3 Théorème de division

Comme on en a parlé dans la partie 1.2, on veut définir une division euclidienne sur $\mathbb{Z}[i]$ afin d'utiliser toutes les propriétés arithmétiques et algébriques d'un anneau principal. On veut définir la division euclidienne sur $\mathbb{Z}[i]$ avec la norme N comme le stathme euclidien :

$$\forall (\alpha, \beta) \in \mathbb{Z}[i] \times \mathbb{Z}[i] \setminus \{0_{\mathbb{Z}[i]}\},\ \exists \gamma, \rho \in \mathbb{Z}[i],\ \textit{tels que}\ \alpha = \beta\gamma + \rho\ \wedge\ N(\rho) < N(\beta).$$

On va expliciter le méthode pour trouver de tels γ et ρ avec un exemple.

Exemple 3.3.1. Soient $\alpha = 24+15i$, $\beta = 1+7i$. Comme la division usuelle sur $\mathbb{Z}[i]$, on prend d'abord le ratio :

$$\frac{\alpha}{\beta} = \frac{24+15i}{1+7i} = \frac{(24+15i)(1-7i)}{(1+7i)(1-7i)} = \frac{129-168i}{50} = 2+\frac{29}{50} - (3+\frac{18}{50})i = \Re(\frac{\alpha}{\beta}) + \Im(\frac{\alpha}{\beta}).$$

Posons $\gamma := n+mi$. Si on prend γ tel que $|n|$, $|m|$ sont les plus grands comme sur $\mathbb{Z}$,

$$\alpha = \beta\gamma + \rho \iff (1+7i)(2-4i) + (-6+5i) = 24+15i, N(-6+5i) \geq N(1+7i)$$

alors $N(\rho) \geq N(\beta)$, donc cela n'a pas de sens pour la division euclidienne. Pour que l'on évite de tels problemes, on propose un version modifié de la division euclidienne : on prend le plus proche intéger de $\Re(\frac{\alpha}{\beta})$, $\Re(\frac{\alpha}{\beta})$ pour $\Re(\gamma)$, $\Im(\gamma)$ tel que :

$$\alpha = \beta\gamma + \rho \iff (1+7i)(3-3i) + (-3i) = 24+15i, N(-3i) < N(1+7i),$$

ce qui nous donne le résultat voulu. Plus rigoreusement, on peut dire que l'on privilégie $\gamma \in \mathbb{Z}[i]$ tel que $N(\rho) = N(\alpha - \beta\gamma) \leq (1/2)\beta$ dans la division euclidienne "modifiée". Ce choix particulier de quotient nous donne quelques caractérisques intéressantes sur le résultat de division, à savoir :

- Le reste peut etre négatif.
- Il n'y a pas d'unicité de quotient et de reste (c.f. exemple 3.3.3).

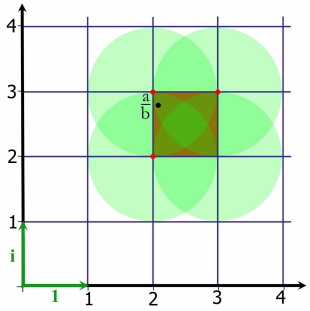

FIGURE 1 – Division euclidienne sur $\mathbb{Z}[i]$
(image par wikipédia)

Ici, a/b est à une distance inférieure à 1 des trois entiers de Gauss $2+2i$, $2+3i$ et $3+3i$; ce qui nous atteste qu'il n'y a pas d'unicité de la solution de la division euclidienne.

On résume l'existence de la division euclidienne sur $\mathbb{Z}[i]$ avec le théorème suivant :

Théorème 3.3.2 (Théorème de division). Soient $(\alpha, \beta) \in \mathbb{Z}[i] \times \mathbb{Z}[i] \setminus \{0_{\mathbb{Z}[i]}\}$. Il existe $\gamma, \rho \in \mathbb{Z}[i]$ tels que $\alpha = \beta\gamma + \rho$ et $N(\rho) < N(\beta)$. En effet, on peut réduire la norme de ρ jusqu'a $N(\rho) \leq 1/2N(\beta)$.

Démonstration. Soient $(\alpha, \beta) \in \mathbb{Z}[i] \times \mathbb{Z}[i] \setminus \{0_{\mathbb{Z}[i]}\}$. On cherche $\gamma, \rho \in \mathbb{Z}[i]$ tels que $\alpha = \beta\gamma + \rho$ et $N(\rho) < N(\beta)$. Prenons d'abord le ratio de α/β :

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} := \frac{m+ni}{N(\beta)}.$$

Avec la division euclidienne "modifiée" de $m, n \in \mathbb{Z}$ par $N(\beta)$, on peut écrire $m = N(\beta)q + r$, $n = N(\beta)q' + r'$ avec $0 \leq |r|, |r'| \leq 1/2N(\beta)$ et $r, r', q, q' \in \mathbb{Z}$. Alors on a :

$$\frac{\alpha}{\beta} = \frac{(N(\beta)q + r) + (N(\beta)q' + r')i}{N(\beta)} = (q+q'i) + \frac{r+r'i}{N(\beta)}.$$

Posons $\gamma := q + q'i \in \mathbb{Z}[i]$. On aura :

$$\alpha = \gamma\beta + \frac{r + r'i}{\bar{\beta}} \iff \alpha - \gamma\beta = \frac{r + r'i}{\bar{\beta}} := \rho \in \mathbb{Z}[i].$$

Montrons que $N(\rho) := N(\alpha - \gamma\beta) \leq 1/2N(\beta)$. On a :

$$N(\alpha - \gamma\beta) = N(\frac{r + r'i}{\bar{\beta}}) \iff N(\alpha - \gamma\beta) = \frac{r^2 + r'^2}{N(\beta)}.$$

Comme on a pris $r, r' \in \mathbb{Z}$ tels que $0 \leq |r|, |r'| \leq 1/2N(\beta)$,

$$N(\alpha - \gamma\beta) = \frac{r^2 + r'^2}{N(\beta)} \leq \frac{(1/2N(\beta))^2 + (1/2N(\beta))^2}{N(\beta)} = \frac{1/2N(\beta)^2}{N(\beta)} = 1/2N(\beta).$$

□

On termine par quelques exemples qui nous attestent qu'il n'y a pas d'unicité de solutions de la division euclidienne sur $\mathbb{Z}[i]$.

Exemple 3.3.3. Soient $\alpha = 1 + 8i, \beta = 2 - 4i$. On a :

$$\frac{\alpha}{\beta} = \frac{1 + 8i}{2 + 4i} = \frac{(1 + 8i)(2 + 4i)}{(2 - 4i)(2 + 4i)} = \frac{-30 + 20i}{20} = -\frac{3}{2} + i.$$

Comme $-3/2$ est exactement au milleu de -1 et -2, on peut utiliser les deux pour la partie réelle du quotient ; soient $\gamma_1 = -1+i, \gamma_2 = -2+i$. On peut obtenir $\alpha-(-1+i)\beta = -1 + 2i = \rho_1, \alpha - (-2 + i)\beta = 1 - 2i = \rho_2$.

Exemple 3.3.4. Soient $\alpha = 37 + 2i, \beta = 11 + 2i$. On a :

$$\frac{\alpha}{\beta} = \frac{37 + 2i}{11 + 2i} = \frac{(37 + 2i)(11 - 2i)}{(11 + 2i)(11 - 2i)} = \frac{411 - 52i}{125} = (3 + \frac{36}{125}) - (0 + \frac{52}{125})i.$$

Donc par la division euclidienne "modifiée", on aura $\gamma = 3, \rho = \alpha - 3\beta = 4 - 4i$. Or, on on peut trouver aussi la solution $\alpha = (3 - i)\beta + (2 + 7i)$ tel que $N(2 + 7i) \leq 1/2N(\beta)$ sans le méthode de division euclidienne "modifiée" generalisé.

3.4 Algorithme d'Euclide sur $\mathbb{Z}[i]$

Dans cette partie, on va parler de l'une des propriétés remarquables qui est donnée par l'existence de la division euclidienne sur $\mathbb{Z}[i]$: l'algorithme d'Euclide. En effet, cette propriété fonctionne presque identiquement sur $\mathbb{Z}$; on commence en définissant les notions de pgcd de deux éléments et de nombres premiers entre eux sur $\mathbb{Z}[i]$.

Définition 3.4.1. Soient $\alpha, \beta \in \mathbb{Z}[i]^*$. Un *plus grand commun diviseur* de α et β est un diviseur commun de α et β avec la norme maximale.

Définition 3.4.2. Soient $\alpha, \beta \in \mathbb{Z}[i]^*$. Alors α et β sont *premiers entre eux* si et seulement si la norme de $pgcd(\alpha, \beta)$ est égale à 1.

Avec ces définitions, on introduit le théorème de l'algorithme d'Euclide ; la démonstration est laissée au lecteur car elle est identique à celle sur $\mathbb{Z}$.

Théorème 3.4.3 (Algorithme d'Euclide). Soient $\alpha, \beta \in \mathbb{Z}[i]^*$. On applique le théorème de division récursivement ; en commençant par (α, β) et en prenant le diviseur et le

reste comme les nouveaux dividende et diviseur, on répète la procédure jusqu'à ce que le reste devienne nul.

$$\begin{aligned}
\alpha &= \beta\gamma_1 + \rho_1,\ N(\rho_1) < N(\beta) \\
\beta &= \rho_1\gamma_2 + \rho_2,\ N(\rho_3) < N(\rho_2) \\
&\vdots \\
\rho_{n-2} &= \rho_{n-1}\gamma_n + \rho_n,\ N(\rho_n) < N(\rho_{n-1}) \\
\rho_{n-1} &= \rho_n\gamma_{n+1} + 0,\ N(0) < N(\rho_n)
\end{aligned}$$

Le dernier reste non-nul ρ_n est divisible par tous les diviseurs communs de α et β, et est lui-même est un diviseur commun, donc un $pgcd(\alpha, \beta)$.

Comme la division euclidienne sur $\mathbb{Z}[i]$, il n'y a pas d'unicité sur le résultat d'algorithme sur $\mathbb{Z}[i]$.

Exemple 3.4.4. Soient $\alpha = 5 + 7i, \beta = 5 - 7i$. On a :

$$\begin{aligned}
5 + 7i &= (5 - 7i)i + (-2 + 2i),\ N(-2 + 2i) < N(5 - 7i) \\
5 - 7i &= (-2 + 2i)(-3) + (-1 - i),\ N(-1 - i) < N(-2 + 2i) \\
-2 + 2i &= (-1 - i)(-2i) + 0,\ N(0) < N(-1 - i) \\
&\textit{ou} \\
5 + 7i &= (5 - 7i)i + (-2 + 2i),\ N(-2 + 2i) < N(5 - 7i) \\
5 - 7i &= (-2 + 2i)(-3 + 1) + (1 + i),\ N(1 + i) < N(-2 + 2i) \\
-2 + 2i &= (1 + i)(2i) + 0,\ N(0) < N(1 + i)
\end{aligned}$$

Donc $pgcd(\alpha, \beta) = 1 + i$ à la mulplication par unités près.

On termine cette partie en remarquant quelques conséquences intéressantes pour le pgcd et l'algorithme d'Euclide.

Théorème 3.4.5. Soient $a, b \in \mathbb{Z}$, impairs et premiers entre eux. Posons $c := (b + a)/2$, $d := (b - a)/2$. Alors $c + di$ et $c - di$ sont premiers entre eux sur $\mathbb{Z}[i]$.

Démonstration. Soient $a, b, c, d \in \mathbb{Z}$ tels que a et b sont impairs et premiers entre eux et $c := (b + a)/2$, $d := (b - a)/2$. Soit $n \in \mathbb{Z}$. Supposons que n divise c et d. On a :

$$\begin{aligned}
n \mid c \wedge n \mid d &\implies n \mid (c + d) \wedge n \mid (c - d) \\
&\implies n \mid a \wedge n \mid b \\
&\implies pgcd(c, d) = 1
\end{aligned}$$

car $pgcd(a, b) = 1$.
Comme a et b sont impairs, un de c ou d est pair et l'autre est impair, c'est-à-dire $c^2 + d^2 = N(c + di) = N(c - di)$ est impair.
Posons $m \in \mathbb{Z}[i]$ un diviseur commun de $c + di$ et $c - di$. Alors si m divise $c + di$ la norme de m divise celle de $c + di$ aussi, ce qui implique que $N(m)$ est impair. Cela nous donne :

$$\begin{aligned}
m \mid (c + di) \wedge m \mid (c - di) &\implies m \mid (c + di) + (c - di) \wedge m \mid (c + di) - (c - di) \\
&\implies m \mid 2c \wedge m \mid 2di \\
&\implies N(m) \mid N(2c) \wedge N(m) \mid N(2di) \\
&\implies N(m) \mid c^2 \wedge N(m) \mid d^2 \ \ car\, N(m) = m^2\, est\, impair \\
&\implies N(m) = 1 \ \ car\, pgcd(c, d) = 1.
\end{aligned}$$

$\therefore m \in \mathbb{Z}[i]^\times$. □

Remarque. Soient $\alpha, \beta, \delta \in \mathbb{Z}[i]^*$. Si δ est un $pgcd(\alpha, \beta)$, $N(\delta)$ divise $N(\alpha)$ et $N(\beta)$. Attention, $N(\delta)$ n'est pas forcément le $pgcd(N(\alpha), N(\beta))$, i.e. $\alpha = 4 + 5i$, $\beta = 4 - 5i$; $N(\delta) = 1$ mais $N(\alpha) = N(\beta)$. Donc on a $pgcd(N(\alpha), N(\beta)) = 1 \implies N(\delta) = 1$ avec la réciproque fausse.

Corollaire 3.4.6. Soient $\alpha, \beta, \delta \in \mathbb{Z}[i]^*$ tels que $\delta = pgcd(\alpha, \beta)$ est obtenu par l'algorithme d'Euclide. Alors tout $pgcd(\alpha, \beta)$ est de la forme de $\gamma\delta$ avec $N(\gamma) = 1$.

Démonstration. Soit $\delta' = pgcd(\alpha, \beta)$. Alors $\delta' \mid \delta$, on peut écrire $\delta = \delta'\gamma$ avec $\gamma \in \mathbb{Z}[i]$. On a donc $N(\delta) = N(\delta')N(\gamma) \geq N(\delta')$. Or, comme $\delta' = pgcd(\alpha, \beta)$, $N(\delta')$ est le plus grand parmi les normes des diviseurs communs, i.e. $N(\delta) \leq N(\delta')$.
$\therefore N(\delta) = N(\delta') \implies N(\gamma) = 1.$ □

Remarque. Le corollaire 1 implique que les pgcds sont uniques à la mulplication par unités près sur $\mathbb{Z}[i]$, i.e. $\forall \alpha, \beta \in \mathbb{Z}[i]^\times$, $\exists!\, pgcd(\alpha, \beta)$.

3.5 Les éléments premiers dans $\mathbb{Z}[i]$

Proposition 3.5.1 (admise). Puisque $\mathbb{Z}[i]$ est principal car euclidien, un élément de $\mathbb{Z}[i]$ est irréductible si et seulement si il est premier.
Sans l'hypothèse d'anneau principal, la véracité du sens direct tombe à l'eau.

Théorème 3.5.2. Si la norme d'un entier de Gauss est premier dans $\mathbb{N}$, alors cet entier de Gauss est premier dans $\mathbb{Z}[i]$.

Démonstration. Soient $z \in \mathbb{Z}[i]$ et $p = N(z)$ premier dans $\mathbb{N}$. On pose $z = \beta\gamma$. Ainsi, $N(z) = N(\beta)N(\gamma) = p$. Or p est premier donc $N(\beta) = 1$ ou $N(\gamma) = 1$ donc β est une unité ou γ est une unité donc z n'admet pas de diviseurs non triviaux et il est premier dans $\mathbb{Z}[i]$. □

Théorème 3.5.3. Tout entier de Gauss $z \in \mathbb{Z}[i]$ tel que $N(z) \geqslant 2$ est produit d'entiers de Gauss premiers.

Démonstration. On le démontre par récurrence. Si $N(z) = 2$, z est premier d'après le théorème précédent ; il est produit de lui-même (premier) et d'une unité qui est irréductible par définition, donc premier, donc c'est bon. Si $N(z) \geqslant 3$, supposons que tout entier de Gauss de norme entre 2 et $N(z) - 1$ soit produit d'entiers de Gauss premiers. S'il n'y a pas d'entiers de Gauss de norme $N(z)$, il n'y a rien à montrer, supposons donc qu'il en existe. Parmi eux, si il y en a des premiers, on est ramenés au cas de l'initialisation, supposons alors qu'il y en ait un non premier. Dans ce cas, on écrit $z = \beta\gamma$ où $N(\beta), N(\gamma) \leqslant N(z) - 1$ (car si une des deux normes vaut celle de z, alors l'autre vaut 1 or ici le cas est exclu). Par hypothèse de récurrence, β et γ sont premiers et z est donc un produit d'entiers de Gauss premiers. □

Définition 3.5.4. Dans un anneau A quelconque, on définit un <u>*élément premier*</u> comme un élément $p \in A$ vérifiant, pour $a_1, ..., a_r \in A$

$$p \mid a_1 \cdots a_r \quad \implies \quad \exists j \in [\![1, r]\!], \;\; p \mid a_j.$$

Ici, plus simplement, on parlera d'entier de Gauss premier lorsque l'on aura affaire à un $z \in \mathbb{Z}[i]$ qui ne peut être cassé qu'en des éléments de la forme ± 1, $\pm i$, $\pm z$ ou $\pm iz$.

Remarque. C'est normalement la définition d'un élément irréductible mais on a vu que dans $\mathbb{Z}[i]$ ces deux notions se confondent du fait que l'anneau est principal.

Théorème 3.5.5. La factorisation en entiers de Gauss premiers de $z \in \mathbb{Z}[i]$ de norme $N(z) > 1$ est unique à permutation et unités près.

Démonstration. On le montre par récurrence. Si $N(z) = 2$, on sait déjà que z est premier, donc sa factorisation est unique à permutation et unités près. Si $N(z) \geqslant 3$, et que l'on suppose que les entiers de Gauss de norme entre 2 et $N(z)-1$ admettent une factorisation unique. Supposons qu'il existe des entiers de Gauss de norme $N(z)$, car sinon il n'y a rien à montrer, et intéressons-nous à un composé z de norme $N(z)$. On écrit

$$z = \pi_1 \cdot \pi_2 \cdots \pi_r = \pi'_1 \cdot \pi'_2 \cdots \pi'_s. \tag{1}$$

Si $\pi_1 \mid z$, on a $\pi_1 \mid \pi'_1 \cdot \pi'_2 \cdots \pi'_s$ donc il existe $j \in [\![1, s]\!]$ tel que $\pi_1 \mid \pi'_j$. Quitte à renommer, on peut supposer $j = 1$, soit $\pi_1 \mid \pi'_1$. Or π'_1 est premier donc $\pi_1 = u\pi'_1$ pour $u \in \{\pm 1, \pm i\}$. On réécrit donc (1) comme

$$z = u\pi'_1 \cdot \pi_2 \cdots \pi_r = \pi'_1 \cdot \pi'_2 \cdots \pi'_s,$$

soit, en simplifiant par π'_1

$$z' = u\pi_2 \cdots \pi_r = \pi'_2 \cdots \pi'_s.$$

Et on a $N(z') = N\left(\dfrac{z}{\pi'_1}\right) = \dfrac{N(z)}{N(\pi'_1)} < N(z)$ quitte là aussi à renommer π'_1 pour assurer cette inégalité.
De plus, $u\pi_2$ est premier donc on a deux factorisations de z' en entiers de Gauss premiers. Et comme $N(z') < N(z)$, par hypothèse de récurrence β admet une factorisation unique dans le sens où l'on a $r - 1 = s - 1$ donc on obtient $r = s$ et en réitérant on voit que tous les éléments premiers sont deux à deux égaux à unité près. Cela conclut donc la preuve. □

4 Applications sur $\mathbb{Z}$

Nous allons dans cette partie présenter une preuve du théorème des deux carrés de Fermat s'appuyant sur les propritétés de $\mathbb{Z}[i]$.

Théorème 4.1. Si un nombre premier $p \in \mathbb{Z}^+$ se décompose sous la forme $p = a^2 + b^2$ avec $a, b \in \mathbb{Z}^+$, alors a et b sont uniques.

Démonstration. On considère un nombre premier $p \in \mathbb{Z}^+$ avec $p = a^2 + b^2$. On a donc $p = (a + ib)(a - ib)$ et $N(a + ib) = N(a - ib) = p$. On en déduit d'après 3.5.2 que $a \pm ib$ est premier dans $\mathbb{Z}[i]$.
On considère une autre décomposition $p = c^2 + d^2$. Par factorisation unique, on a $a + ib = u(c \pm di)$ avec $u \in \{\pm 1, \pm i\}$. Sans perte de généralité, on considère le cas $a + ib = u(c + id)$:

$$\begin{aligned}
&\text{Si } \ u = 1, \ \ a = c \ \text{ et } \ b = d \\
&\text{Si } \ u = -1, \ \ a = -c \ \text{ et } \ b = -d \\
&\text{Si } \ u = i, \ \ a = -d \ \text{ et } \ b = c \\
&\text{Si } \ u = -i, \ \ a = d \ \text{ et } \ b = -c
\end{aligned}$$

On a donc l'égalité à l'ordre et au signe près. □

Théorème 4.2. (Théorème de Wilson) (admis) Un entier $n \geq 2$ est premier si et seulement si $(n-1)! \equiv -1 \mod n$.

Démonstration. La demestrontion, assez classique, se trouve dans le TD de l'UE 2MA220.

Lemme 4.3. Un nombre premier $p \in \mathbb{Z}^+$ n'est pas premier dans $\mathbb{Z}[i]$ si et seulement s'il est somme de deux carrés dans $\mathbb{Z}$.

Démonstration. Soit $p \in \mathbb{Z}^+$. Si p n'est pas premier dans $\mathbb{Z}[i]$, on considère la factorisation $p = \alpha\beta$ pour $\alpha, \beta \in \mathbb{Z}[i]$. On a donc :

$$\begin{aligned} N(p) &= N(\alpha\beta) \\ p^2 &= N(\alpha)N(\beta) \end{aligned}$$

Or la factorisation n'est pas triviale et $N(\alpha), N(\beta) \in \mathbb{Z}^+$ donc $N(\alpha) = N(\beta) = p$. En écrivant $\alpha = a + ib$, on a :

$$\begin{aligned} p &= N(\alpha) \\ p &= a^2 + b^2 \end{aligned}$$

Supposons maintenant que $p = a^2 + b^2$ avec $a, b \in \mathbb{Z}$. On a alors $p = (a + ib)(a - ib)$ ce qui implique que p n'est pas premier dans $\mathbb{Z}[i]$. □

Théorème 4.4. (Théorème des deux carrés de Fermat) Soit $p \in \mathbb{Z}^+$ un nombre premier. Les assertions suivantes sont équivalentes :

(1) $p = 2$ ou $p \equiv 1 \mod 4$.

(2) L'équation $x^2 \equiv -1 \mod p$ admet des solutions.

(3) $p = a^2 + b^2$ avec $a, b \in \mathbb{Z}$.

Démonstration.
(1) $\implies$ (2) : Si p est premier et $p \equiv 1[4]$, on pose $p = 2k + 1$. D'après le théorème de Wilson on a :

$$\begin{aligned} (p-1)! &\equiv -1 \mod p \\ (p-1) \cdot 1 \cdot (p-2) \cdot 2 \cdots (p-k) \cdot k &\equiv -1 \mod p \\ (-1) \cdot 1 \cdot (-2) \cdot 2 \cdots (-k) \cdot k &\equiv -1 \mod p \end{aligned}$$

Où la dernière ligne est simplement un réarrangement des termes. On en déduit ensuite :

$$\begin{aligned} \prod_{i=1}^{k} i^2 &\equiv (-1)^{k+1} \mod p \\ (k!)^2 &\equiv (-1)^{k+1} \mod p \end{aligned}$$

Si $p \equiv 1 \mod 4$ alors k est pair. On a donc $(k!)^2 \equiv -1 \mod p$. Si $p = 2$, on a $1^2 \equiv -1 \mod p$. L'équation admet donc des solutions.

(2) $\implies$ (3) : Pour montrer ce point, on montre que (2) implique que p n'est pas premier dans $\mathbb{Z}[i]$ ce qui d'après le lemme 4.1.3. implique qu'il est somme de deux carrés. On a :

$$\begin{aligned} & x^2 \equiv -1 \mod p \\ \iff & x^2 + 1 \equiv 0 \mod p \\ \iff & p \mid x^2 + 1 \\ \iff & p \mid (x + i)(x - i) \end{aligned}$$

Supposons maintenant que p est premier dans $\mathbb{Z}[i]$. D'après le lemme d'Euclide sur $\mathbb{Z}[i]$, $p \mid (x+i)$ *ou* $p \mid (x-i)$. On en déduit

$$\exists m, n \in \mathbb{Z},\ p \cdot (m+ni) = x \pm i.$$

On a $pm + pni = x \pm i$ donc par identification, $pn = \pm 1$ ce qui est absurde. On en conclut que p n'est pas premier dans $\mathbb{Z}[i]$. D'après le lemme 4.3., $p = a^2 + b^2$ pour $a, b \in \mathbb{Z}[i]$ ce qui conclut ce point de la preuve.

(3) $\Longrightarrow$ (1) : Si $p = a^2 + b^2$ avec $a, b \in \mathbb{Z}$, on a $p \equiv a^2 + b^2 \mod 4$.

Si $a = 2k$ avec $k \in \mathbb{Z}$, on a :

$$\begin{aligned} a^2 &\equiv 4k^2 \mod 4 \\ a^2 &\equiv 0 \mod 4 \end{aligned}$$

Si $a = 2k+1$ avec $k \in \mathbb{Z}$, on a :

$$\begin{aligned} a^2 &\equiv 4k^2 + 4k + 1 \mod 4 \\ a^2 &\equiv 1 \mod 4 \end{aligned}$$

Donc $p \equiv 0, 1, 2 \mod 4$ or $p \equiv 0$ est impossible car p est premier. Le cas $p \equiv 2$ à lieu seulement si $p = 2$, sinon p n'est pas premier. On en déduit donc $p = 2$ ou $p \equiv 1 \mod 4$. □

Remarque. Le 5-ème nombre de Fermat $2^{2^5} + 1$ n'est pas premier d'après le théorème 4.1.1. car on peux le decomposer sous la forme $2^{2^5} + 1 = (2^{16})^2 + 1^2 = 62264^2 + 20449^2$.